SHARE FOUNDATION

BIRN BALKAN INVESTIGATIVE REPORTING NETWORK

Politikat dhe protokollet e medias

Mbrojtja e të dhënave personale dhe siguria digjitale

Prill **2022**

Përkthimi në shqip është bërë i mundur falë projektit 'Paper Trail to Better Governance' i financuar nga Austrian Development Agency, një njësi operacionale e Austrian Development Cooperation.
Mars 2024

Austrian Development Cooperation

Mbrojtja e të dhënave personale

Udhëzimet

Politika e privatësisë është një dokument që duhet të krijohet me qëllim të ofrimit të informacionit për publikun se pse dhe në çfarë mënyre operatori përdor dhe përpunon të dhënat personale të atyre njerëzve.

Detyrimi për të informuar vjen nga detyrimi ligjor i operatorit [1] për t'u dhënë paraprakisht informacione të përcaktuara me ligj personave, të dhënat e të cilëve ua mbledhin. Në mënyrë që informacioni i kërkuar të jetë i disponueshëm për personat e interesuar paraprakisht, praktika standarde është që politika e privatësisë të publikohet në faqen e internetit të operatorit.

Teksti më poshtë është një shembull i një formulari me të cilin operatori mund të përshkruajë përpunimin e të dhënave personale që ata mbledhin përmes faqes së tyre të internetit në kuadër të politikës së privatësisë. Titujt e këtij shembulli ndjekin informacionin e detyrueshëm që operatori është i detyruar të sigurojë sipas Ligjit për Mbrojtjen e të Dhënave Personale dhe rregulloreve tjera në fuqi.

Në fusnota ka shpjegime se si të përshtatet ky shembull për nevojat e një operatori specifik. Në këtë kuptim, është e nevojshme të futet informacioni që është i rëndësishëm për operatorin specifik brenda çdo pike (titull), duke përfshirë informacionin se disa gjëra nuk përpunohen. Pas përfundimit të tekstit me informacionin e nevojshëm, fusnotat duhet të fshihen.

Nëse operatori nuk mbledh të dhëna personale, rekomandohet të publikohet një njoftim ku kjo specifikohet në faqen e internetit.

Një shembull i një politike specifike të privatësisë që është zhvilluar në përputhje me këto rekomandime, e cila është zhvilluar nga Fondacioni SHARE nga Serbia, mund të gjendet këtu.

[1] Çdo organ publik, person fizik ose juridik, agjenci ose organ tjetër që në mënyrë të pavarur ose së bashku me të tjerët kryen, përpunon dhe përcakton qëllimin dhe metodën e përpunimit të të dhënave personale bazuar në ligje ose rregullore.

Politika e Privatësisë

Në tekstin e mëposhtëm, mund të informoheni se në cilat situata, për çfarë qëllime dhe në çfarë mënyre operatori i listuar më poshtë përpunon të dhënat personale, duke marrë parasysh informacionin që operatorët janë të detyruar të paraqesin sipas dispozitave të ligjit.[2]

1) Identiteti dhe detajet e kontaktit të operatorit

<Emri>
<Adresa>
<Qyteti, Vendi>

2) Detajet e kontaktit të operatorit në lidhje me mbrojtjen e të dhënave personale

<ofroni detajet e kontaktit >

3) Qëllimi i përpunimit, burimi i të dhënave dhe baza ligjore për procesim[3]

Qëllimi[4]	***Lloji[5] dhe burimet e të dhënave[6]***	***Baza ligjore[7]***
<deklaroni qëllimin e përpunimit të të dhënave >	<specifikoni mënyrat e mbledhjes dhe burimet e të dhënave për këtë qëllim >	<specifiko bazën ligjore për përpunimit e të dhënave për këtë qëllim >
<deklaroni qëllimin e përpunimit të të dhënave>	<specifikoni mënyrat e mbledhjes dhe burimet e të dhënave për këtë qëllim >	<specifikoni bazën ligjore për përpunimin e të dhënave për këtë qëllim >

[2] Modeli i paraqitur në këtë kapitull duhet të koordinohet me të dhënat e sakta personale që organizata që punon në krijimin e politikave të privatësisë është e detyruar të paraqesë, në përputhje me Ligjin për Mbrojtjen e të Dhënave Personale të atij vendi.

[3] Informacioni nën këtë titull mund të jepet në formë teksti ose tabele. Në dokumentin përfundimtar, është e nevojshme të fshihet tabela, pra teksti narrativ, varësisht se cila prej dy formave është informacioni i dhënë nën këtë titull.

[4] Qëllimi mund të jetë, për shembull: komentimi në faqen e internetit; plotësimi i formularit të kontaktit në faqen e internetit; pjesëmarrja në anketa; abonimi në buletin; regjistrimi në faqen e internetit; donacionet për operatorin etj.

[5] Llojet e të dhënave mund të jenë, për shembull: emri; adresa elektronike; telefoni; adresa IP; përmbajtja e një komenti ose mesazhi; numri i llogarisë bankare etj.

[6] Të dhënat mund të mblidhen drejtpërdrejt nga personi që ia ofron operatorit - për shembull nga personi që sapo i ka futur ato në faqe, ose në mënyrë indirekte - për shembull, nga burime të disponueshme publike.

[7] Baza ligjore e përpunimit mund të jetë pëlqimi i personit, interesi legjitim i operatorit, një kontratë që operatori ka me personin ose përmbushja e detyrimeve ligjore të operatorit. Nëse nuk jeni të sigurt, duhet të konsultoheni me një avokat lidhur me bazën e duhur ligjore.

apo

< në formën e një teksti narrativ, tregoni/përshkruani veçmas çdo qëllim, informacion se si janë mbledhur të dhënat për të përmbushur atë qëllim dhe, nëse është e nevojshme, çfarë të dhënash janë, si dhe cila është baza ligjore për secilin qëllim.>

4) Marrësit e të dhënave personale[8]

Operatori ndan të dhëna personale me <specifiko marrësin e të dhënave, p.sh. organizatat me të cilat ndahen të dhënat >.

5) Transferimi i të dhënave personale në një vend tjetër[9]

Të dhënat personale janë përpunuar në <specifiko vendin ku ruhen të dhënat>.

6) Periudha e ruajtjes së të dhënave personale, p.sh. kriteret për përcaktimin e tyre[10]

<specifikoni periudhën e ruajtjes së të dhënave, d.m.th. momentin pas të cilit të dhënat fshihen dhe, nëse ka qëllime të shumta, është e nevojshme të specifikohen afate të ndryshme për secilin nga qëllimet e përpunimit>.

7) Të drejtat e personave të cilëve u referohen të dhënat

Çdo person të cilit i referohen të dhënat që ne përpunojmë, ka të drejtë të kërkojë nga operatori:

- T'i informojë ata me vërtetësi dhe plotësisht për përpunimin e të dhënave të tyre;
- Të drejtën për qasje dhe/apo një kopje të të dhënave që u referohen atyre;
- Të drejtën për të korrigjuar dhe shtuar të dhëna të pasakta ose të paplota, në çdo kohë;
- Të drejtën e fshirjes, e cila mund të jepet në përputhje me kushtet ligjore, pra kur: të dhënat personale nuk janë më të nevojshme për të arritur qëllimin për të cilin janë mbledhur ose përpunuar në mënyra tjera; personi të cilit i referohen të dhënat ka paraqitur një kundërshtim për përpunimin bazuar në interesin legjitim të operatorit dhe nuk ka asnjë bazë tjetër ligjore për procesim;

[8] Vendosni marrësit e të dhënave, me të cilët operatori ndan të dhënat (për hir të mirëkuptimit, rekomandohet të specifikoni arsyen për të cilën ndahen të dhënat). Këta mund të jenë bashkëpunëtorë biznesi, kompani ose organizata të lidhura biznesi, shërbime korriere, konsulentë ligjorë dhe financiarë, autoritete shtetërore kompetente, etj. Nëse nuk ka marrës me të cilët ndahen të dhënat personale, duhet të shkruhet në këtë titull.

[9] Futni informacione se në cilat shtete përpunohen të dhënat. Nëse është e nevojshme, kontrolloni se ku është vendosur faqja e internetit. Nëse të dhënat përpunohen në vende që nuk konsiderohen adekuate sipas rregulloreve përkatëse, tregoni bazën ligjore për transferimin e të dhënave në vendet joadekuate.

Për shembull: *Të dhënat personale përpunohen në Serbi dhe Indi. Transferimi i të dhënave në Indi, i cili nuk konsiderohet një vend që ofron një nivel adekuat të mbrojtjes së të dhënave, rregullohet dhe sigurohet nga Klauzola Standarde Kontraktuale.*

[10] Shembuj të periudhës së ruajtjes mund të jenë: të dhënat personale që jepni kur lini një koment ruhen përgjithmonë, d.m.th. ato nuk fshihen si vetë komentet; adresa elektronike që keni dhënë për të marrë buletinin fshihet kur të çregjistroheni; të dhënat që jepni në formularin e kontaktit në faqen e internetit ruhen për një maksimum prej një viti pas dërgimit të mesazhit.

- Të dhënat personale janë përpunuar në mënyrë të paligjshme; të dhënat personale duhet të fshihen për të përmbushur detyrimet ligjore të operatorit;
- Të drejtën për të kufizuar përpunimin, e cila mund të përmbushet nëse plotësohen kushtet e kërkuara: nëse personi të cilit i referohen të dhënat ka kundërshtuar saktësinë e të dhënave personale dhe operatorit i duhet kohë që i lejon atij të kontrollojë saktësinë; nëse përpunimi është i paligjshëm, dhe personi kundërshton fshirjen dhe në vend të fshirjes kërkon kufizimin e përdorimit të të dhënave; operatori nuk ka më nevojë për të dhënat personale për të arritur qëllimin e përpunimit, por personi i ka kërkuar ato me qëllim paraqitjen, realizimin ose mbrojtjen e një pretendimi ligjor; ose personi ka paraqitur tashmë një kundërshtim për përpunimin dhe po bëhet një vlerësim nëse baza ligjore për përpunimin nga operatori tejkalon interesat e personit;
- Transferimin e të dhënave në formë të lexueshme nga makinat, e cila ekziston në rastet kur është e zbatueshme, d.m.th nëse është teknikisht e mundur sepse të dhënat janë të lexueshme nga makina dhe kur baza ligjore për përpunim është pëlqimi i personit ose një marrëdhënie kontraktuale me personin të cilit i referohen të dhënat;
- Të drejtën për të tërhequr pëlqimin e tyre për përpunimin e të dhënave të caktuara në çdo kohë, nëse pëlqimi është një bazë ligjore për përpunim.

Personi gjithashtu ka të drejtë të kundërshtojë, nëse personi të cilit i referohen të dhënat konsideron se interesi legjitim i operatorit në bazë të të cilit përpunohen të dhënat nuk justifikohet, domethënë se kërcënon të drejtat, lirinë dhe interesat e atij personi.

Në rast të përpunimit të automatizuar të të dhënave personale dhe vendimmarrjes, personi ka të drejtën e ndërhyrjes njerëzore, si dhe të drejtën të shprehë mendimin e tij për vendimin ose të kundërshtojë vendimin.

8) E drejta për të bërë ankesë

Personi ka të drejtë të paraqesë një ankesë kundër veprimeve të operatorit pranë autoritetit kompetent në përputhje me ligjin e vendit në të cilin operatori operon.

9) Ekzistenca e vendimmarrjes së automatizuar, duke përfshirë profilizimin[11]

Operatori nuk kryen vendimmarrje të automatizuar, as profilizim, bazuar në të dhëna personale.

[11] Mediat zakonisht nuk kryejnë profilizimin (krijimin e profileve unike) dhe vendimmarrjen e automatizuar për të drejtat dhe interesat e vizitorëve në faqet e tyre të internetit (marrja e vendimeve pa ndërhyrjen njerëzore, por vetëm përmes "algoritmeve"). Nëse operatori ende e bën këtë, është e nevojshme të shpjegohen qartë dhe kuptueshëm qëllimet dhe mënyrat në të cilat kryhet një përpunim i tillë.

[12] Nëse përdorni cookie që mund të çojnë në identifikimin e drejtpërdrejtë ose të tërthortë të përdoruesve të caktuar të faqes tuaj të internetit (nëpërmjet ndonjë identifikuesi unik), përdorimi i cookieve të tillë konsiderohet gjithashtu si përpunim i të dhënave personale.
Në atë rast, së pari ju duhet të përcaktoni nëse ka ndonjë cookie për të cilën keni një interes legjitim për t'i përdorur (të tilla si cookie rreptësisht të nevojshme), që në atë rast është një bazë ligjore për përpunimin e të dhënave. Të gjitha cookie-t e tjera mund të përdoren vetëm në bazë të pëlqimit të vizitorit të faqes së internetit. Prandaj, atëherë është e nevojshme dhe rekomandohet që të aktivizoni një opsion pop-up, në të cilin vizitorët e faqes në internet do të kenë mundësinë të refuzojnë të gjitha cookie-t që nuk mund të justifikohen nga interesi, siç janë skedarët analitikë, marketingu dhe skedarët e palëve të treta.

10) Politika e Cookie[12]

<u><Në këtë titull, jepet vetëm një shembull se si operatori mund të përshkruajë përdorimin e cookies në faqen e tyre të internetit. Nëse dëshironi të përdorni tekstin e mëposhtëm, ai duhet të përshtatet me faqen specifike të internetit >.</u>

Një "cookie" është një pjesë e vogël e të dhënave që një faqe interneti mund të dërgojë në shfletuesin tuaj, e cila më pas mund të ruhet në hard diskun tuaj. Nëse jeni të shqetësuar për privatësinë tuaj dhe përdorimin e teknologjisë "cookie", mund të vendosni shfletuesin tuaj që t'ju njoftojë kur të merrni një "cookie". Cookies mund t'ju ndihmojnë të jeni më efikas dhe të përfitoni nga funksionet "memorie", për shembull kur një faqe interneti kujton gjuhën tuaj në të cilën e keni parë faqen nga një vizitë e mëparshme. Cookies ju lejojnë të ruani preferencat tuaja, të ruani produkte dhe shërbime dhe të personalizoni faqet.

Operatori përdor cookies në faqen e tij për të ofruar shërbime dhe funksionalitet për përdoruesit e tij. Ju mund të kufizoni ose çaktivizoni përdorimin e cookies përmes shfletuesit tuaj të internetit, por pa cookies nuk do të jeni në gjendje të përdorni të gjitha funksionet e faqes.

Ekzistojnë lloje të ndryshme të cookie-ve dhe sipas kritereve se kush i vendos cookies në faqen e internetit, ne i dallojmë:

- cookie-t e palës së parë – cookies të vendosura nga operatori kur përdorni faqen e internetit; dhe
- cookie-t e palëve të treta – cookies të vendosura nga një organizatë tjetër kur përdorni faqen e internetit (disa faqe interneti mund të përmbajnë gjithashtu përmbajtje nga sajte të tjera që mund të vendosin skedarët e tyre të personalizimit).

Për sa i përket qëllimit, ne përdorim llojet e mëposhtme të cookies në faqe:

- Cookies Rreptësisht të Nevojshme – Këto cookie janë të nevojshme për të menaxhuar statusin tuaj të lidhjes.
- Cookies Funksionale – këto cookies lejojnë faqen e internetit të kujtojë veprimet tuaja të mëparshme në mënyrë që t'ju ofrojë funksione të avancuara.
- Cookies Analitike – këto cookie na lejojnë të mbledhim të dhëna për përdorimin tuaj të faqes së internetit në mënyrë që të përmirësojmë performance dhe dizajnin e saj. Për të çaktivizuar cookie e Google Analytics, shkarkoni dhe instaloni këtë shtojcë (this plugin).
- Cookies të marketingut – këto cookie përdoren për të mbledhur informacione të ndryshme në lidhje me vizitën tuaj në faqen tone, të tilla si informacione në lidhje me përmbajtjen që keni parë, lidhjet që keni ndjekur, shfletuesin tuaj, pajisjen ose IP adresën.

Siguria digjitale

Politikat e brendshme të sigurisë

Siguria digjitale është e një rëndësie kyçe për organizatat mediatike dhe individët që i përbëjnë ato, pra gazetarët dhe punonjësit e tjerë, si dhe burimet me të cilat gazetarët vijnë në kontakt gjatë hulumtimit. Për ta bërë më të sigurt përdorimin e teknologjisë gjatë punës së tyre, mediat duhet të miratojnë politika dhe procedura të përshtatshme që do t'i ndihmojnë në këtë. Në rast incidentesh teknike, të tilla si një sulm në një faqe interneti mediatike ose marrja e llogarisë, këto politika mund të ndihmojnë në parandalimin ose të paktën minimizimin e dëmtimit të burimeve të një organizate.

Në varësi të kapacitetit dhe burimeve të organizatës, krijimi i politikave të sigurisë së brendshme përfshin pjesëmarrjen e menaxhmentit, stafit redaktues, anëtarëve të ekipit përgjegjës të IT, si dhe gazetarëve dhe punonjësve të tjerë që zotërojnë aftësi teknike më të avancuara që ata mund t'i bartin te të tjerët. Trajnimi dhe edukimi i punonjësve është i rëndësishëm për zbatimin e procedurave dhe politikave pa prishur proceset e rregullta të punës.

Çdo dokument i brendshëm në fushën e sigurisë digjitale duhet t'u përshtatet nevojave dhe aftësive reale të organizatës, për të qenë i saktë dhe i kuptueshëm për të gjithë të interesuarit. Politikat e brendshme duhet të jenë të disponueshme në formë elektronike vetëm për anëtarët e ekipit, pra jo për publikun. Për këto qëllime, mund të përdoret një platformë për komunikim të brendshëm si Mattermost, Rocket.Chat, Element në mënyrë që punonjësit, në rast dyshimi ose që punojnë jashtë ambienteve të organizatës, të kenë qasje në dokumentacion dhe të konsultohen me kolegët ose personat përgjegjës për monitorimin e zbatimit të politikave, p.sh. redaktorët.

Shembuj të dokumenteve të brendshme janë politika e fjalëkalimit, politika për përdorimin e adresave zyrtare të postës elektronike dhe llogarive shoqëruese, si dhe plani i sigurisë.

Politika e fjalëkalimeve

Qëllimi i dokumentit të mëposhtëm është t'i ndihmojë organizatat të krijojnë një politikë unike për përdorimin dhe menaxhimin e fjalëkalimeve, në mënyrë që të ofrohen procedura të qarta. Politika e fjalëkalimit i mundëson organizatës dhe anëtarëve të saj të krijojnë, përdorin, ruajnë dhe modifikojnë në mënyrë të sigurt fjalëkalime të cilat përfaqësojnë mekanizmin bazë të vërtetimit, d.m.th. mbrojtjen e burimeve të organizatës nga qasja e paautorizuar..

_____(Emri i organizatës)

1. Kjo politikë zbatohet për fjalëkalimet e përdorura për të mbrojtur llogaritë, pajisjet, dokumentet, bazat e të dhënave dhe burime tjera të menaxhuara nga _____(Emri i organizatës).

2. Një fjalëkalim i vetëm nuk duhet të përdoret për të mbrojtur burime të shumëfishta të ndryshme. Fjalëkalimet nuk duhet të shfaqen publikisht ose të ndahen me persona të paautorizuar.

3. Nëse ekziston një mundësi teknike, është e nevojshme të futet verifikimi i dyfishtë (verifikimi me 2 hapa) për çdo burim të menaxhuar nga _____(Emri i organizatës).

4. Ndryshimi i të gjitha fjalëkalimeve për burimet e menaxhuara nga _____ (Emri i organizatës) është bërë për një periudhë prej ____muaj.

5. Fjalëkalimet duhet të jenë të paktën 15 karaktere të gjata, duhet të përmbajnë karaktere të veçanta (p.sh. shenja pikësimi), shkronja të mëdha, shkronja të vogla dhe numra. Fjalëkalimet nuk duhet të përmbajnë të dhëna personale të punonjësve (p.sh. emrat, mbiemrat, datat e lindjes, numrat e telefonit, adresat e banimit) ose të personave të afërt me ta (p.sh. anëtarët e familjes së ngushtë).

6. Për burime veçanërisht të ndjeshme (p.sh. bazat e të dhënave që përmbajnë të dhëna të një natyre veçanërisht të ndjeshme: viktima të dhunës, statusi shëndetësor, orientimi seksual, etj.) është e nevojshme të futen fraza mbrojtëse (fraza kalimi) që përbëhen nga vargje fjalësh të zgjedhura rastësisht në kombinim me të tjera të detyrueshme elementet për fjalëkalimet nga pika 5 e kësaj politike. Frazat e sigurisë duhet të jenë të paktën 20 karaktere të gjata.

7. Person i përgjegjës në organizatë për administrimin e fjalëkalimeve është _____(emri dhe mbiemri, vendi i punës).

8. Me caktimin e një fjalëkalimi për llogaritë që përdoren për punën dhe aktivitetet e (Emri i organizatës), siç janë llogaritë zyrtare të postës elektronike, punonjësve u kërkohet të ndryshojnë fjalëkalimin e dhënë në përputhje me këtë politikë menjëherë pasi ta marrin atë nga personi kompetent i cili krijoi llogarinë (p.sh. administrator teknik) dhe ia caktoi punonjësit. Fjalëkalimet e reja duhet të krijohen dhe ruhen në një menaxhues fjalëkalimesh.

9. Fjalëkalimet dhe frazat e sigurisë ruhen në aplikacione speciale të destinuara ekskluzivisht për

menaxhimin e fjalëkalimeve (p.sh. KeePass, KeePassXC) që ruajnë bazën e fjalëkalimit në kujtesën lokale të pajisjes. Ruajtja e fjalëkalimeve në shfletuesit e internetit dhe në faqet e ruajtjes së fjalëkalimeve në internet nuk lejohet.

10. Bërja e një kopje rezervë të bazës së të dhënave të fjalëkalimeve të ruajtura në një memorie të jashtme (p.sh. hard disk i jashtëm, USB) bëhet sa herë që ndryshohen fjalëkalimet dhe frazat e sigurisë (duke shtuar të reja ose duke ndryshuar të vjetrat) dhe duhet të tregohet data kur është krijuar në emrin e skedarit

11. Në rast se një punonjës vëren ose dyshon se ndonjë burim i menaxhuar nga_____ (Emri i organizatës) është kompromet uar, ata do të informojnë menjëherë mbikëqyrësin e tyre dhe do të ndryshojnë fjalëkalimin ose frazën e sigurisë për atë burim, dhe nëse është një burim i përbashkët, ata do të njoftojnë personin në organizatën përgjegjëse për administrimin e fjalëkalimit.

12. Politika hyn në fuqi __ditë pas miratimit të tij.

Datë: _____ Personi i autorizuar nga organizata:_____
Vendi: _____

Politika për përdorimin e postës elektronike dhe llogarive shoqëruese

Udhëzimet

Duke përdorur dokumentin e mëposhtëm, organizatat mund të krijojnë një politikë unike për përdorimin dhe menaxhimin e llogarive zyrtare të postës elektronike dhe llogarive të lidhura me të (d.m.th. paketat e plota të shërbimit të produktivitetit të ofruara nga ofruesit si Google ose Microsoft) në mënyrë që të jetë e qartë për çfarë qëllimesh mund të përdoren, kujt i janë caktuar, si të veprojnë gjatë largimit të anëtarëve të ekipit nga organizata dhe të ngjashme. Politika e llogarisë u mundëson organizatave dhe anëtarëve të tyre të menaxhojnë llogaritë në pronësi të organizatës në mënyra që reduktojnë rreziqet e mundshme brenda sigurisë digjitale dhe t'i përdorin ato në përputhje me qëllimet e përcaktuara.

Emri dhe adresa e organizatës

Politika e përdorimit të adresës elektronike dhe llogarisë përcjellëse _____(Emri I organizatës)

Kjo politikë përmban kushtet për përdorimin e postës elektronike dhe llogarive shoqëruese në domenet e internetit në pronësi të _____, përkatësisht: _____(futni domenet, p.sh. organizacija.rs) (në tekstin e mëposhtëm: domenet _____).

1. Adresa elektronike dhe llogaritë përcjellëse të krijuara për qëllime të punës, praktikës dhe vullnetarizmit në_____janë në pronësi të _____.
2. _____administron llogaritë dhe i lëshon për përdorim personave që janë të punësuar në_____, personat që janë në praktikë dhe për vullnetarët.
3. Personi të cilit i është lëshuar llogaria e postës elektronike përdor llogarinë dhe _____ nuk ka njohuri mbi përmbajtjen e asaj llogarie ose pjesëve mbështetëse (ruajtjes në cloud, dokumentet bashkëpunuese, etj.).
4. Llogaritë në domene _____përdoren ekskluzivisht për qëllimet e specifikuara nga _____.
5. Në rast të ndërprerjes së marrëdhënies në mes të _____dhe personit të cilit i është lëshuar llogaria, pronësia e llogarisë mbetet e _____.
6. _____do të lërë një periudhë 30 ditëshe nga data e ndërprerjes së marrëdhënies, për personin të cilit i është lëshuar llogaria për të mbledhur të gjithë përmbajtjen për të cilën mendojnë se do t'ju nevojitet nga llogaria.
7. Pas skadimit periudhës 30 ditëshe nga përfundimi i marrëdhënies, llogaria do të fshihet, dhe një kopje e përmbajtjes do të arkivohet për qëllim të _____.
8. Politika hyn në fuqi në datën e miratimit.
9. Personave të cilëve u janë caktuar llogaritë do të njoftohen për çdo ndryshim të ardhshëm të kësaj politike.

Vendi dhe data, Personi përgjegjës

Plani i sigurisë

Plani i sigurisë ka për qëllim që t’i ndihmojë organizatat që krijojnë masa parandaluese dhe reaguese në lidhje me incidentet teknike, të marrin në konsideratë rreziqet dhe kërcënimet e mundshme për infrastrukturën teknike të organizatës, të përshkruajnë procedura dhe hapa në rast të trajtimit të llojeve të ndryshme të incidenteve teknike, etj. Ndërsa nuk është e mundur të parashikohet çdo skenar i vetëm i sulmit teknik, duke pasur një plan sigurie mund të parandalojë ose minimizojë dëmet dhe të ndihmojë në rikuperim.

Kur të krijoni një plan të sigurisë, konsideroni hapat si vijon:

Qëllimet: vendos një qëllim primar realist ose disa qëllime dytësore, në mënyrë që masat e përcaktuara të zbatohen realisht për të arritur qëllimet e dhëna.

Kërcënimet dhe rreziqet: mendoni për skenarët e mundshëm të kërcënimeve ndaj sigurisë digjitale të organizatës suaj dhe anëtarëve të saj, kjo do t'ju ndihmojë të identifikoni më saktë kërcënimet dhe rreziqet e mundshme për sigurinë digjitale dhe të përgatiteni më mirë për t'u marrë me to.

Hapat parandalues: listoni hapat realistë që mund të ndërmerrni kur bëhet fjalë për mbrojtjen e sigurisë digjitale, duke marrë parasysh kërcënimet, rreziqet dhe kapacitetet e vetë organizatës (teknike, organizative dhe të personelit).

Hapat në rast incidenti: merrni parasysh skenarët e mundshëm të incidentit (p.sh. marrja e paautorizuar e llogarive të mediave sociale) dhe përcaktoni hapat e nevojshëm në situata të caktuara. Ndonëse nuk është realiste të parashikohen të gjithë skenarët, zgjidhni disa që mendoni se janë më realiste të ndodhin ose që i kanë ndodhur tashmë organizatës suaj.

Pajisjet dhe mjetet e rekomanduara: Krijoni një listë të zgjidhjeve harduerike dhe softuerike që kanë reputacion të mirë dhe rekomandohen nga komuniteti i ekspertëve. Merrni parasysh kapacitetet e organizatës dhe nëse nuk jeni të sigurt se çfarë do t'i përshtatet më mirë nevojave tuaja, kërkoni këshilla të jashtme.

Aplikimi i procedurave të brendshme: Përshkruani në mënyrë specifike zbatimin e procedurave tuaja të sigurisë për disa shembuj të incidenteve që ju besoni se janë më realiste të ndodhin ose që keni përjetuar më parë në organizatë.

Plani i sigurisë

QËLLIMI	Përmirësoni sigurinë digjitale të organizatës në tërësi dhe individëve brenda saj
KËRCËNIMET DHE RREZIQET	• Kompromet imi i të dhënave personale dhe i informacionit konfidencial (dokumentet, korrespondencat…) • Kompromet imi i burimeve dhe infrastrukturës teknike të organizatës • Humbja e kontrollit mbi infrastrukturën dhe të dhënat
HAPAT PARANDALUES	• Qasja në infrastrukturën dhe burimet e organizatës (serverët, pajisjet e rrjetit, llogaritë në rrjetet sociale, panelet e administrimit të faqeve të internetit, etj.) e mundësuar vetëm për persona të caktuar dhe e mbrojtur me fjalëkalime të forta të ruajtura në aplikacione të veçanta për këtë qëllim (menaxherët e fjalëkalimeve, p.sh. KeePass) • Politika të adoptuara nga organizata për fjalëkalime • Verifikim i dyfishtë (verifikim me 2-hapa) duke i përfshirë të gjitha llogaritë që e mbështesin atë • Mbani të koduara të dhënat veçanërisht ato të ndjeshme (p.sh. informacionin për viktimat e dhunës seksuale), në pajisje speciale që nuk përdoren për punë të përditshme • Pajisjet e të punësuarve të mbrojtura me fjalëkalime /pin kode • Ruajtja e rregullt e të dhënave në pajisjet lokale (p.sh. hard disqe të jashtme) dhe/apo online (në serverin e organizatës apo në shërbimet në cloud, p.sh. Dropbox, Google Drive, OneDrive...). **Megjithatë, veçanërisht të dhënat personale dhe informacionet tjera konfidenciale nuk duhet të ruhen në shërbimet cloud.** • Përdorni adresa elektronike të koduara (PGP) dhe aplikacione për biseda (Signal) për të këmbyer informacione konfidenciale.

HAPAT NË RAST INCIDENTI	• Njoftoni sa më shpejt kolegët kompetentë (administratorët përgjegjës për infrastrukturën teknike në organizatë) dhe mbështetjen teknike (p.sh. kompaninë pritëse) dhe ndiqni udhëzimet e tyre • Mblidhni të gjitha informacionet e disponueshme rreth incidentit (koha, vendi, aktivitetet gjatë incidentit, adresat IP, regjistrat, pamjet e ekranit, konfigurimet e fundit të sakta...) në mënyrë që të përcaktohen dëmet dhe dëmtimet • Njoftoni ekipet speciale/sektoriale të reagimit ndaj incidenteve kibernetike, të tilla si CERT Kombëtare (Ekipi i Reagimit ndaj Emergjencave Kompjuterike) • Raportojeni incidentin tek autoritetet kompetente shtetërore • Kontrolloni versionin e fundit të disponueshëm të konfigurimit të të dhënave/sistemit për të tentuar të ktheheni në gjendjen e mëparshme dhe të rindërtoni
PAJISJET DHE MJETET E REKOMANDUARA	• Telefona celularë me aplikacione të instaluara të enkriptuara për biseda (Signal) • Kompjuterët: softuerë antivirus të instaluar dhe përditësuar rregullisht, si dhe të gjitha programet e tjera të përdorura • Kompjuterët: të instalohet menaxheri i fjalëkalimeve (p.sh. KeePass, KeePassXC) • Kompjuterët: të instalohet softueri për enkriptimin e harduerit (VeraCrypt) • Të krijohen çelësa PGP për adresat elektronike të punëtorëve dhe të instalohet softueri adekuat (p.sh. Thunderbird, Gpg4Win, Mailvelope) • Shfletuesit (Browsers): Mozilla Firefox, të instalohen plug-in (HTTPS Everywhere, Privacy Badger, uBlock Origin, minerBlock, Facebook Container) apo Brave në të cilët versionet e Google Chrome plug-in mund të instalohen • Në pajisje instalohet një VPN i besueshëm (p.sh. Mullvad, ProtonVPN) dhe Tor Browser

APLIKIMI I PROCEDURAVE TË BRENDSHME (SHEMBULL)	Punëtorët kanë vënë re se faqja e internetit të organizatës nuk është e disponueshme ose ka vështirësi të ngarkohet 1. Kontrolloni disponueshmërinë e faqes në shërbimin "Jashtë funksionit për të gjithë apo vetëm për mua" (https://downforeveryoneorjustme.com/) dhe lidhjen e internetit 2. Skanoni të gjithë kompjuterët dhe pajisjet me një softuer antivirus 3. Nëse konstatohet se nuk është problem teknik, punonjësi informon personalisht ose nëpërmjet një kanali të sigurt komunikimi (bisedë sinjalizuese, mesazh adresë elektronike të koduar) administratorin teknik të organizatës. 4. Administratori, në bashkëpunim me mbështetjen teknike, kryen kontrollin e infrastrukturës dhe nëse konstatohet se ka pasur trafik të pazakontë, qasje të paautorizuar ose shkelje të tjera të integritetit të sistemit të informacionit, mbledh prova digjitale. 5. Hapi tjetër është një përpjekje për të rivendosur funksionalitetin e të dhënave/rikthimit duke përdorur kopje rezervë dhe/ose konfigurime e mira të fundit 6. Pas kësaj është përcaktimi i llojit të sulmit dhe kualifikimet ligjore, njoftimi i organeve kompetente dhe përgatitja e parashtresave (p.sh. kallëzimet penale) në bashkëpunim me ekipet speciale/sektoriale.